Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A cryptographic system in a computer system, comprising:

at least one server including a key repository process;

a database coupled to the server for storing sensitive information, the integrity of the database is maintained by an integrity key and the sensitive information is managed by the key repository process, the key repository process also validates and records authorizations of applications to access the sensitive information; and

at least one secret value including a master key for protecting the sensitive information, the master key being split into two or more parts wherein fewer than all the parts are required for reassembling the master key using the key repository process, the parts being encrypted by a password-derived or token-based key, each part being associated with a password wherein the at least one server can update the master key by requiring only some of the passwords to be revealed.

2. (Cancelled).

3. (Cancelled).

4. (Original) A cryptographic system as in claim 1 in which the master key is split into the two or more parts according to the Bloom-Shamir methodology.

5. (Currently amended) A method used in a cryptographic system including a server, comprising:

providing a database for storing sensitive information;

providing at least one secret value including a master key;

splitting the master key into two or more parts wherein fewer than all the parts are required for reassembling the master key; ~~and~~

encrypting the parts by a password-derived or token-based key, each part being associated with a password and stored in the database; and

using a key repository process for managing the sensitive information in the database, the key repository process using an integrity key to maintain the integrity of the database and ~~wherein~~ the master key can be reassembled by the ~~server~~ key repository process by requiring only some of the passwords to be revealed.

6. (Previously presented) A method as in claim 5, wherein the master key is used for protecting sensitive information processed by the server in the cryptographic system.

7. (Original) A method as in claim 5 wherein the master key is split into the two or more parts according to the Bloom-Shamir methodology.

8. (Currently amended) A server, comprising:

a storage area for storing a at least one secret value including a master key, the master key being split into two or more parts wherein fewer than all the parts are required for reassembling the master key, the parts being encrypted by a password-derived or token-based key, each part being associated with a password;

a key repository process for managing information in the storage area using an integrity key for protecting the integrity of the storage area and the master key for protecting sensitive information in the database; and

means for updating the master key by requiring only some of the passwords to be revealed.

9. (Previously presented) A server as defined in claim 8, further comprising an input coupled to the means for updating the master key, the input receiving some of the passwords.

10. (Previously presented) A server as defined in claim 9, wherein some of the passwords are received from a plurality of clients coupled to the server.